

Prepared Remarks S.B. S.B. 283, S.B. 668, H.B. 6100, and H.B. 6111

Government Administration and Elections Committee
Testimony – February 22, 2013

Luther Weeks
Luther@CTVotersCount.org
334 Hollister Way West, Glastonbury, CT 06033

Chairs and members of the Committee, my name is Luther Weeks, Executive Director of CTVotersCount, an experienced Certified Moderator, a Computer Scientist, and a Veteran.

I have submitted written testimony on four bills. I appreciate questions on any them, but will use most of my three minutes for S.B. 283.

It is Risky, Expensive, likely Unconstitutional, Ineffective, and Discriminatory.

Here, I will emphasize several relevant issues raised in my written testimony and in the hearings three days ago in Veterans' Affairs for S.B. 647.

- Internet Voting Is Risky In Theory and in Practice. In only one case has an online voting system been subject to an independent security test. Although too brief, that test of a system identified several vulnerabilities. Washington D.C. should to be applauded for allowing the test and for cancelling that system.
- This is an Expensive, Unfunded Mandate: Waterloo, Canada estimated Internet voting would cost \$300,000 per election over their current election costs of \$400,000. West Virginia spent about \$75,000 for 54 electronic Military votes. Often cited as a success, West Virginia has yet to implement online voting since the prototype in 2010.
- This Bill Is Likely Unconstitutional: Tuesday I kept hearing of a voter's option to waive their right to a secret vote. That right does not exist and misunderstands the purpose of a secret ballot.

The Connecticut Constitution says that *"The right of secret voting shall be preserved."* i.e. it is a guarantee that everyone's votes shall be anonymous, protected from coercion and purchase.

- Conventional, Safe Solutions Are Available:
 - On Tuesday, no one expressed awareness of free USPS express mail return of ballots available to military voters. We can fix that.
 - Rhode Island officials testified that only 53 of 1 700 of their voters used fax and email return. Were Connecticut as successful as Rhode Island and West Virginia, we could expect our return rate to increase, at most, from 60% to 63.2%.

S.B 283, like H.B. 6100 and H.B6111, is a brief description of an insufficiently defined, complex concept. The devil will be in the details:

- Who will be responsible for its implementation and management?
- How will we pay for it? Via unfunded mandate?
- Exactly what is meant by "online" voting, even experts disagree.

Thank you

Chairs and members of the Committee, my name is Luther Weeks, Executive Director CTVotersCount, an experienced, Certified Moderator, a Computer Scientist, and a Veteran.

I applaud this Committee for holding hearings on this Risky, Expensive, likely Unconstitutional, Ineffective, and Discriminatory bill. Last year this Committee held no hearings on this concept and stuck an even worse concept far down in an unrelated emergency bill.

In addition, this bill suffers from a being brief description, insufficiently defined. The devil will be in the details – this bill should have those details available for registrars, town clerks, and advocates to review and publicly testify for or against such details. Who would be responsible for implementing it? How will we pay for it?

- **Internet Voting Is Risky In Theory:** The Computer Technologists Statement on Internet Voting details five technical challenges to such voting that have never been resolved and concludes: *“The internet has the potential to transform democracy in many ways, but permitting it to be used for public elections without assurance that the results are verifiably accurate is an extraordinary and unnecessary risk to democracy.”*
- **Internet Voting Has Proven Risky In Practice:** In September 2010, Washington D.C. opened their proposed internet voting system to ethical hackers. With very short notice, the system was compromised, changing all past and future votes. Separately, the municipal network was entered, passwords to municipal systems obtained, and the list of codes for Internet voting for all voters in the November election were obtained. Internet voting for the election was cancelled. Washington D.C. should be applauded for allowing the test, since most other jurisdictions have not subjected their systems to such testing. Just recently, a user compromised a test in Edmonton, Canada. <http://tinyurl.com/CT2013sb283>
- **This is an Expensive, Unfunded Mandate:** Waterloo, Canada estimated Internet voting would cost \$300,000 per election over their current election costs of \$400,000. West Virginia spent about \$75,000 for 54 electronic Military votes. Often cited as a success, West Virginia has yet to continue online voting since the prototype in 2010.
- **This Bill Is Discriminatory:** Many overseas voters are veterans but not members of the Military. Some serve in remote areas or challenging conditions. Including: State Department, CIA, and NGO staffs, plus Military Contractors, and Peace Corps volunteers. .
- **This Bill Is Likely Unconstitutional:** The Connecticut Constitution says that *“The right of secret voting shall be preserved.”* i.e. it is a guarantee that everyone’s votes shall be anonymous, protected from coercion and purchase. Network communications can be intercepted, web entry can be monitored.
- **This bill Is Ineffective:** On Tuesday, Veterans’ Affairs heard testimony on S.B. 647 for email and fax voting that, sadly only 60% of ballots requested by Connecticut’s military were successfully returned. Yet also testimony from Rhode Island officials that only 53 of 1700 of their voters used fax and email return. If Connecticut were equally successful with online military voting, we could expect our return rate to increase, at most, from 60% to 63.2%.

- **There Are Move Effective, Safer, and Economical Alternatives Available:** Conventional solutions for effective, safe, and economical Military voting are available and proven. Let us exploit the MOVE Act and help our overseas military voter take full advantage of free or prepaid express ballot return.

I oppose this bill in particular because:

- **It contains no controls, specifications, or requirements for online voting.** Would there be any public testing of such systems? Would there be any attempt to address the Techologists's concerns or prevent problems similar to those in Washington, D.C?
- **What entity would be responsible for implementing it?** It does not specify if such voting would be the responsibility of individual municipalities or the Secretary of the State.
- **How would we pay or it?** It provides no funds either for the State or Municipalities to implement.
- **Could Connecticut accomplish centrally what Washington D.C. has not? Would each of Connecticut's 169 municipalities be able to afford such systems and accomplish what Washington D.C. has not?**
- **Would the system be optional by municipality? Different in each municipality? If implemented in only some, would it be unfair, violating Federal civil rights and voting laws?**

Please join me, computer scientists, security experts, and advocates nationwide in opposing online and Internet voting in any form.

Failing that, at least provide the funds and a mandate to require such a system be subject to contracted evaluation and testing by recognized independent network security experts, and open to extensive public testing, at least as open as the tests in Washington, D.C – before such a system is trusted with actual votes.

There is no need to applaud my military service. Yet, there will be every reason to applaud your service, if you drop this bill. It is an affront to the ideals for which all of our veterans and ancestors have given so much.

Thank you

"If I can shop and bank online, why can't I vote online" by David Jefferson,
Computer Scientist, Lawrence Livermore National Laboratory, Board Chairman, Verified Voting
Foundation, Board of Directors, California Voter Foundation
<http://electionlawblog.org/wp-content/uploads/jefferson-onlinevoting.pdf>

Free express mail ballot return for overseas military:

"Uniformed Services personnel, their voting age dependents and civilians stationed overseas may Express return their absentee ballots FREE of charge from any APO/FPO/DPO, American embassy or consulate with this label".
http://www.fvap.gov/resources/media/mpsa_poster.pdf

View the video of the Secretary of the State Denise Merrill's Symposium On Online Voting, held for the benefit of the General Assembly, with Nationally recognized experts on Internet voting:
<http://ctvoterscount.org/secretary-of-the-states-online-voting-symposium/>

Waterloo, Canada estimates online voting will add \$300,000 to current election costs of \$400,000. And the risks of the similar system in Edmonton
<http://ctvoterscount.org/if-it-feels-good-do-it-in-canada/>

Edmonton, Canada. Concerns, costs, and compromise of test of an expensive vendor system.
<http://ctvoterscount.org/CTVCdata/13/01/Leader20130204.pdf>

<http://tinyurl.com/EdRejects>

EDMONTON JOURNAL

Edmonton council defeats proposal for Internet voting this fall

- The future of Internet voting in Alberta is unclear after Edmonton city council turned down a proposal Wednesday to allow online ballots as part of October's civic election.

Although city staff insisted the system was extensively tested over the past year, including a mock "jelly bean" election and confirmation by a citizen jury, councillors worried the process isn't entirely secure.

"The fact is, if major banks can be hacked, what's guaranteeing our voting system wouldn't be hacked?" Coun. Kerry Diotte asked.

There were also fears someone could collect other voters' email addresses, picture identification and passwords, then cast multiple ballots in a hotly contested race.

"If you want to coerce someone, it's easier to do that with Internet voting than it is at a voting station," Coun. Tony Caterina said.

"At this point in 2013, I don't think you're ready to answer all these questions."

There was little support for the initial proposal to permit Internet ballots before the Oct. 21 election in advance polls, which attracted 15,000 people in 2010.

But council voted 11-2 against a compromise motion to allow it just for special ballots, used three years ago by about 800 shut-ins, election workers and people away from Edmonton for an extended period.

Don Iveson and Ben Henderson were the only councillors to favour the move, arguing electronic ballots are as secure as the paper version.

"I think there's, frankly, some paranoia about the technology because it's unknown," Iveson said.

"I understand the instinct to want to test it further, but those risks that people will behave badly aren't going to go away."

City clerk Alayne Sinclair said an outside consulting company was hired to try to breach the jelly bean election system, but along with a NAIT computing class and 10 other hackers, they didn't succeed.

While one computer programmer says he cast two ballots in the mock election, showing it's vulnerable to fraud, he appears to have done this by registering twice, which wasn't being controlled, Sinclair said.

"We were told by the professionals that for all of the time people say they can penetrate the system, there's no example anywhere that anyone has."

Providing Internet ballots would have cost \$400,000.

The city has already paid \$400,000 to test the system developed by Spain's Scytl, but Coun. Linda Sloan had philosophical as well as money concerns.

"Do we really want to configure a system where people can vote in their pyjamas? ... Voting is an act of civic engagement," she said.

"I'm not convinced this is a direction we want to take, particularly because it privatizes both the act and the system of voting."

The province has been working with Edmonton, St. Albert and Strathcona County since last year on how to introduce Alberta's first Internet voting, already used in dozens of centres in Ontario and Nova Scotia.

Grande Prairie, the Regional Municipality of Wood Buffalo, Airdrie, and Lethbridge were also studying the idea.

Officials in the two capital region municipalities don't know what will happen now that their largest partner has backed out.

"The intention of the pilot was to have the three of us do it together," said Jacqueline Roblin, Strathcona County's manager of legislative services.

"Now that Edmonton is no longer on board, I'm not sure how this will proceed."

But Kalina Kamenova, who spent months working on public consultation for the scheme as research director at the University of Alberta's Centre for Public Involvement, said she thinks city council made the wrong decision.

Most councillor concerns were already addressed by the 17-member citizen jury, which after days of discussions and hearing from experts supported online voting, Kamenova wrote in an email.

"It is surprising that councillors went against the verdict of the citizen jury and overlooked Edmontonians' overwhelming support for this innovative voting option," she wrote, emphasizing this is her opinion.

"It makes you wonder why so much money is being spent by the city for public involvement when citizens' input doesn't really have any impact on decision-making."

© Copyright (c) The Edmonton Journal

Computer Technologists' Statement on Internet Voting

Election results must be *verifiably accurate* -- that is, auditable with a permanent, voter-verified record that is independent of hardware or software. Several serious, potentially insurmountable, technical challenges must be met if elections conducted by transmitting votes over the internet are to be verifiable. There are also many less technical questions about internet voting, including whether voters have equal access to internet technology and whether ballot secrecy can be adequately preserved.

Internet voting should only be adopted after these technical challenges have been overcome, and after extensive and fully informed public discussion of the technical and non-technical issues has established that the people of the U.S. are comfortable embracing this radically new form of voting.

A partial list of technical challenges includes:

- **The voting system as a whole must be verifiably accurate in spite of the fact that client systems can never be guaranteed to be free of malicious logic.** Malicious software, firmware, or hardware could change, fabricate, or delete votes, deceive the user in myriad ways including modifying the ballot presentation, leak information about votes to enable voter coercion, prevent or discourage voting, or perform online electioneering. Existing methods to "lock-down" systems have often been flawed; even if perfect, there is no guaranteed method for preventing or detecting attacks by insiders such as the designers of the system.
- **There must be a satisfactory way to prevent large-scale or selective disruption of vote transmission over the internet.** Threats include "denial of service" attacks from networks of compromised computers (called "botnets"), causing messages to be mis-routed, and many other kinds of attacks, some of which are still being discovered. Such attacks could disrupt an entire election or selectively disenfranchise a segment of the voting population.
- **There must be strong mechanisms to prevent undetected changes to votes,** not only by outsiders but also by insiders such as equipment manufacturers, technicians, system administrators, and election officials who have legitimate access to election software and/or data.
- **There must be reliable, unforgeable, unchangeable voter-verified records of votes** that are at least as effective for auditing as paper ballots, without compromising ballot secrecy. Achieving such auditability with a secret ballot transmitted over the internet but without paper is an unsolved problem.
- **The entire system must be reliable and verifiable** even though internet-based attacks can be mounted by anyone, anywhere in the world. Potential attackers could include individual hackers, political parties, international criminal organizations, hostile foreign governments, or even terrorists. The current internet architecture makes such attacks difficult or impossible to trace back to their sources.

Given this list of problems, there is ample reason to be skeptical of internet voting proposals. Therefore, the principles of operation of any internet voting scheme should be publicly disclosed in sufficient detail so that anyone with the necessary qualifications and skills can verify that election results from that system can reasonably be trusted. Before these conditions are met, "pilot studies" of internet voting in government elections should be avoided, because the apparent "success" of such a study absolutely cannot show the absence of problems that, by their nature, may go undetected. Furthermore, potential attackers may choose only to attack full-scale elections, not pilot projects.

The internet has the potential to transform democracy in many ways, but permitting it to be used for public elections without assurance that the results are verifiably accurate is an extraordinary and unnecessary risk to democracy.

<http://www.verifiedvotingfoundation.org/article.php?id=6611>

Endorsements [Computer Technologists' Statement on Internet Voting]

The computer technology experts below endorse this statement. Affiliations are for identification only, and do not imply that employers have a position on the statement.

Alex Aiken
Professor of Computer Science, Stanford University

Andrew W. Appel
Professor of Computer Science, Princeton University

Ben Bederson
Associate Professor, Computer Science Department,
University of Maryland

L. Jean Camp
Associate Professor, School of Informatics, Indiana
University

David L. Dill
Professor of Computer Science, Stanford University and
Founder of VerifiedVoting.org

Jeremy Epstein
Software AG and Co-Founder, Verifiable Voting Coalition of
Virginia

David J. Farber
Distinguished Career Professor of Computer Science and
Public Policy Carnegie Mellon University

Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton
University

Michael J. Fischer
Professor of Computer Science, Yale University, and
President, TrueVoteCT.org

Don Gotterbarn
Director, Software Engineering Ethics Research Institute,
Computer and Information Sciences, East Tennessee State
University

Joseph Lorenzo Hall
UC Berkeley School of Information

Harry Hochheiser
Assistant Professor, Computer and Information Sciences,
Towson University

Jim Horning
Chief Scientist, SPARTA, Inc., Information Systems Security
Operation

David Jefferson
Lawrence Livermore National Laboratory

Bo Lipari
Retired Software Engineer, Executive Director New Yorkers
for Verified Voting

Douglas W. Jones
Professor of Computer Science, University of Iowa

Robert Kibrick
Director of Scientific Computing, University of California
Observatories / Lick Observatory

Scott Klemmer
Assistant Professor of Computer Science, Stanford
University

Vincent J. Lipsio

Peter Neumann
Principal Scientist, SRI International

Eric S. Roberts
Professor of Computer Science, Stanford University

Avi Rubin
Professor, Computer Science, Johns Hopkins University

Bruce Schneier
Chief Security Technology Officer, BT Global Services

John Sebes
Co-Director, Open Source Digital Voting Foundation
Chief Technology Officer, TrustTheVote Project

Yoav Shoham
Professor of Computer Science, Stanford University

Barbara Simons
IBM Research (retired)

Eugene H. Spafford
Professor and Executive Director of CERIAS, Purdue
University

Michael Walfish
Assistant Professor of Computer Science, University of
Texas, Austin

Dan S. Wallach
Associate Professor, Department of Computer Science, Rice
University

Luther Weeks
Retired Software Engineer and Computer Scientist

Jennifer Widom
Professor of Computer Science, Stanford University

David S. Wise
Computer Science Dept., Indiana University

S.B. 668 – Support with Suggested Additions

**Government Administration and Elections Committee
Testimony – February 22, 2013**

**Luther Weeks
Luther@CTVotersCount.org
334 Hollister Way West, Glastonbury, CT 06033**

Chairs and members of the Committee, my name is Luther Weeks, Executive Director of CTVotersCount. I am a Certified Moderator, with four years of moderating the central counting of Absentee Ballots in Vernon. I am looking forward to serving voters by supervising the Election Day Registration (EDR) function in Glastonbury this November.

I agree that it is not necessary to train poll workers more than once a year, for the same function. Yet, training for different roles should be required, if not covered in a previous training. For instance, central counting of Absentee Ballots is entirely different than functioning as a poll worker. I suggest the proposed text, at minimum, be changed as follows:

That chapter 146 of the general statutes be amended to require that each poll worker be trained at least once a year, but not required to attend training prior to each election if such training session would result in a poll worker being trained for the same election day role a second time in a calendar year.

Further, it is important that Election Day Registration (EDR) workers be trained. They are not poll workers since the EDR location is not defined in the law as a poll. I would suggest:

That chapter 146 of the general statutes be amended to require that each poll worker and election day registration worker be trained at least once a year, but not required to attend training prior to each election if such training session would result in a poll worker being trained for the same election day role a second time in a calendar year.

Let me reiterate what I have said in the past, that the EDR bill passed last year leaves too much undefined. Let me suggest critical items for your consideration in priority order:

1. It should be mandatory that anyone in line at 8:00pm have the right to have the opportunity to register and vote.
2. The EDR function should require at the very minimum a Certified Moderator and two Assistant Registrars, providing the same protections for potential voters and parties available in a polling place.
3. The EDR function should require privacy booths and adequate space.
4. The EDR function should require posting of everything required to be posted at polling places.
5. EDR votes should be required to be totaled and reported in municipalities and to the Secretary of the State as separate counts
6. The EDR function should also require at least a Trainer, Ballot Clerk, and Ballot Box Tender. EDR locations are required to handle ballots for up to 32 different districts, it would be important to provide each voter the correct ballot and to provide new voters the opportunity to spoil ballots and revote. Presuming most are new voters having a Trainer would serve them.

Conscientious registrars would likely provide many of these items to serve and protect the rights of voters, yet others concerned with tight budgets and criticism for “unnecessary” expenditures might not.

Thank You

H.B. No. 6111 – Oppose as Insufficient to Evaluate

Government Administration and Elections Committee

Testimony – February 22, 2013

Luther Weeks

Luther@CTVotersCount.org

334 Hollister Way West, Glastonbury, CT 06033

Chairs and members of the Committee, my name is Luther Weeks, Executive Director CTVotersCount, a veteran, a Certified Moderator, and a computer scientist.

I support the goal of making it easier for overseas citizens and overseas military members to vote as envisioned by the existing Federal MOVE Act. The Uniform Act (UMOVEA) proposed in H.B.6111, provides some useful additions beyond that act, such as extending several Federal requirements to state and local elections. <http://tinyurl.com/UMOVEA>

However, I do not support this “placeholder” text that does not specify specific choices, options, additions, and deletions from the uniform law. Specific concerns I can identify include:

- The uniform law text has options that each state may or may not include primaries, run-offs, and referendums in the “uniform law”. If any of these are included, absentee ballots must be available 45 days in advance, just as they are in Federal elections. Currently under Sec. 9-369c of the statutes, absentee ballots must be made available three weeks in advance of a referendum and in some circumstances, less. This may pose even more difficult timing challenges, if run-offs are included.**
- Absentee ballot provisions of the current law must be changed to accommodate the act’s requirement that ballots postmarked by 12:01am on the day of the election be counted if received up until one day before latest deadline for reporting final election results. Presumably moderators, head moderators, and counters will have to be available to count such ballots on a date up to 30 days after such elections, since by Connecticut law they alone are responsible for counting absentee ballots. My reading of the statutes is that certification dates are often up to thirty days after elections. This would mean that Connecticut would need to hold primaries even earlier to accommodate this requirement and the 45 day advance ballot availability requirement.**
- The uniform act, unnecessarily expands these risky voting options to include military and military dependents that are not stationed overseas. I recommend that all overseas voters and only overseas military be included in its provisions. Other voters can easily use existing, less risky, absentee ballot provisions.**

Some examples of problems with conflict with current law if the UMOVEA 45 day required advance availability/transmission of ballots is included for some elections, primaries, referendums, and special elections:

- In 2013 there will be 56 days after the September 10th primary and the November 5 election, given that there are only 49 days after the last day to conduct a recanvass of the primary, only 42 days after the last day for filing an election complaint. Currently absentee ballots must be available by October 4th, but under UMOVEA they would need to be available Sept 21st. Thus current law and UMOVEA would be in conflict.**
- In 2012 we had a recanvass and a court challenge in a primary crossing Windsor and Hartford. The challenge was not heard until 17 days after the primary, the court ordered a**

second recanvass 31 days after the primary, which was completed and resolved by other court action 36 days after the election, resulting in a run-off election 50 days after the primary. A similar situation under UMOVEA would make it impossible to provide ballots 45 days in advance for a municipal election.

- In the previous example, if run-offs were included in UMOVEA then the run-off would have required at least a 45 day advance notice. I would have to be held a minimum of 81 days after the election. If a similar process were to occur.
- Sec. 9-369c (and perhaps others) requires at least three week's notice to town clerks for referendums to prepare absentee ballots. That also provides an exemption for referendums with less than three weeks notice, allowing only in-person absentee ballot requests. All these provisions would be in conflict if referendums were included in UMOVEA.
- Sec. 9-215 provides only 46 days from writs for a CT House or Senate vacancy to such election, likely too short to produce ballots 45 days in advance

The best hope of curing these problems and meet the 45 day requirement of UMOVEA would be to move the municipal primaries at least a month earlier. And increase the lead time for referenda or exempting referenda from UMOVEA.

I am only one, election official, only one moderator. Others may find other issues needing attention. I caution against passing this bill without public hearings providing for review and comment on the actual text of a proposed bill – Give election officials and town clerks an opportunity to point out implementation challenges/costs and advocates the opportunity to point out risky or discriminatory details.

Thank You

H.B. No. 6100 – Support with Suggested Function

Government Administration and Elections Committee

Testimony – February 22, 2013

Luther Weeks

Luther@CTVotersCount.org

334 Hollister Way West, Glastonbury, CT 06033

Chairs and members of the Committee, my name is Luther Weeks, Executive Director CTVotersCount.

Since 2007, as Executive Director of the Connecticut Citizen Election Audit Coalition, I have organized voters to observe and independently report on post-election audits. My remarks represent my views, not necessarily the views of other Coalition members.

I support the goal of regional sharing of election resources between municipalities. This would the potential to increase voter service and election integrity, while reducing costs.

The bill suggests “certain functions”, I would like to add a function, with some conditions, that can result in increased election integrity: **“Regional Storage of Voted Ballots”**.

Currently there is uncertainty and inadequacy in the law with regard to the storage and secure retention of voted ballots. The law should be strengthened and clarified. At least for regional consolidation, let us provide stronger protection for voted ballots:

- All voted ballots should be stored to provide **physical security** and **independent records** of all access that assure that they are always secure or under the custody of two individuals of opposing interests. Currently, very few municipalities provide credible protections.

I envision a “vault” type facility with video surveillance - similar to that used in several town halls today. Two authorized individuals of opposing interests presenting identification and their access recorded for permanent retention by an independent official.

- Even without regional storage, voted ballots should have be “locked down” from election day until they are released by the Secretary of the State, after all post-election audit counting an recounting is complete. Currently ballots are only clearly required to be so protected until the day before the post-election audits begin, day 14 after the election.

I have attached a Hartford Courant editorial articulating the need for two people of opposing interests to access ballots, motivated by events in East Haddam in 2009.

As stated in the Connecticut Citizen Audit Coalition Nov 2011 Post-Election Audit Report **<http://www.ctelectionaudit.org/nov-2011-election-audit-observation-report/>**

“Audit and chain-of-custody procedures are not followed. This report does not question any individual’s integrity. However, a safe, credible system of security procedures should not permit a single individual any extended opportunity to handle records and ballots unobserved...”

A larger concern is that, in many towns, single individuals may access the ballots undetected for extended periods of time. In 41% of towns surveyed in this audit, a single individual can access the ballot storage. In other towns, even though policies require more than one person to access ballots, there are little protections to prevent a single person from accessing the ballot storage.”

Thank You

Hartford Courant Editorial

Only One Party Observed Haddam Vote Count

November 23, 2009

The unofficial tally of votes cast in the Nov. 3 election showed Democratic incumbent Sabrina Houlton beating Republican Chester Harris by one vote for a seat on the Haddam board of education. But after a mandatory recount on Nov. 10, the tally showed that Mr. Harris edged out Ms. Houlton by that most slender one-vote margin.

Case closed, right? Not by a long shot.

The next day, when town offices were closed for Veterans Day, head election moderator Marge DeBold, a Democrat, found a clerical error in the absentee vote count that added an additional vote to Ms. Houlton's total. That extra vote would throw the results into a tie, which would require a runoff election. The following day, Democratic Registrar Pat Hess authorized Ms. DeBold and Town Clerk Ann Huffstetler, also a Democrat, to open the sealed envelopes containing the ballots to review the tally sheets and amend the recount.

But there were no Republicans present. That was wrong.

Ms. Hess said she knew representatives from both parties needed to be present during all vote-counting procedures, but the GOP registrar could not attend that morning. What was her feeble excuse for proceeding anyway? The Democrats wanted to complete the new tallies quickly to file the proper paperwork with the secretary of the state's office. There was no intentional wrongdoing, Ms. Hess said.

But there was. The Democrats decided to proceed with verifying the addition of the game-changing one vote without a Republican being present. Even in a small town, even among friends, even when there is no fraud, the rules must be scrupulously followed to maintain trust.

Mr. Harris, the initial winner of the recount, summed it up well: "The process was corrupted. When you go by yourselves, just you two, it gives the appearance of impropriety."

Copyright © 2009, The Hartford Courant

Chain-of-Custody Concerns

Audit and chain-of-custody procedures are not followed. This report does not question any individual's integrity. However, a safe, credible system of security procedures should not permit a single individual any extended opportunity to handle records and ballots unobserved...

In several observations, observers expressed concerns with the chain-of-custody in the several ways. In 5 municipalities observers expressed general concerns with the chain-of-custody. This is about the same percentage (17%) as the two most recent observations with 14% and 18% concerns.

A larger concern is that, in many towns, single individuals may access the ballots undetected for extended periods of time. In 41% of towns surveyed in this audit, a single individual can access the ballot storage. In other towns, even though policies require more than one person to access ballots, there are little protections to prevent a single person from accessing the ballot storage.

Selected observer comments and their record of official responses to survey questions:

- *The ballots are stored as are most town records in file cabinets with a single file cabinet style lock within a single large open room. Despite a very attractive "logging" book they sign together when opening the file cabinet, there is no barrier to a single person opening the cabinet alone*
- *Only one individual returned ballots.*
- *Nothing to prevent just one Registrar opening it – each has a key locked in his desk. Their office is kept locked.*
- *The 2 registrars; there is one shared key, policy and tradition dictate that they access ballots together.*